

NUCLEAR INTELLIGENCE WEEKLY®

Vol. 11, No. 16



April 21, 2017

Special Reprint from *Nuclear Intelligence Weekly* for Stimson Center.
Unauthorized access or electronic forwarding, even for internal use, is prohibited.

IN PERSPECTIVE

So You Think Nuclear Plant Liabilities Are Covered?

*The nuclear liability regime contains many gaps, chief of which is the failure to deal with cyber risks, according to Kathryn Rauhut, an attorney and Stimson nonresident fellow based in Vienna, Austria, and Debra Decker, a Stimson senior advisor based in Washington, DC. The Stimson Center just released a report, *Demonstrating Due Care: Cyber Liability Considerations for Nuclear Facilities*.*

Nuclear industry supporters are eager to allay public fears about the potential for another severe nuclear incident like Fukushima. A major issue is the possibility of extensive damaging consequences and compensation for those losses, with cyber being a topmost concern. The nuclear liability regime, a complicated labyrinth of national laws and treaties, promises victims will be compensated in the event of a severe nuclear incident. But is that true? Not necessarily, according to a panel of legal and insurance experts assembled by the Stimson Center in London last fall. Huge gaps remain, with cyber risks representing one of the greatest holes in the framework.

The nuclear liability framework helped encourage private investment in commercial nuclear power by capping operator liability in the event of an incident. An important feature is channeling of liability to the operator, meant to avoid lengthy litigation to establish legal responsibility and to provide a ready source of funds to compensate victims. But the international and domestic framework with liability caps may be irrelevant in the face of today's range of threats, including perhaps most importantly cyber.

Cyber and terrorism risks have the potential to cause catastrophic economic and personal losses even without causing a release of radiation. Yet in the absence of an event causing a radiation release or authorized evacuation, the US Price-Anderson Act and the international liability regime provide no liability protection or compensation at all. Today the spectrum of risks against which nuclear operators must insure has increased significantly beyond radiation-related harm, which owes in large part to the advent of the cyber age and the new risks it brought with it.

Last November in London, the Stimson Center, along with the Security Awareness Special Interest Group and the World Institute for Nuclear Security (WINS) held the Nuclear Security Roundtable on Executive and Corporate Responsibility. The roundtable brought together fifty industry stakeholders, including lawyers, insurers and cybersecurity experts, to discuss a nuclear power station attack that did not threaten a radiation release. In the scenario, the cyberattack undermined the facility's

security posture, with subsequent physical effects triggering a plant shutdown. As the source of the continuing plant issues could not be easily determined, the plant stayed offline, resulting in a sustained area-wide power outage.

In this instance, nuclear power operators' potential liabilities are like other power generators'. Lloyds' Business Blackout report highlighted the complexity of claims that would be triggered by a successful cyberattack and blackout. Compensation would be required across broad classes of claims including third-party property losses, business interruption, shareholder lawsuits, personal injury, deaths from exposure to heat or cold, accidents and equipment failure.

Although all power suppliers should be concerned, nuclear plants are some of the largest baseload suppliers and are known targets. In areas without a well-integrated grid system or in the many countries without cybersecurity laws and regulations, nuclear power blackout scenarios are even more likely.

Nuclear facility operators would have to look to their conventional insurance policies to cover losses. Some insurers have inserted certain cyber exclusions into policies. Separate cyber policies are then needed, but caps on those have been low. And although some countries have terrorism risk insurance, not all do. In those that do provide such government-backed insurance, the coverage is uneven.

How can or should nuclear operators address these challenging areas of coverage and non-coverage – and how can owners and managers protect not only their operations but also themselves as lawsuits can get personal?

Just more than a year ago, three former Tokyo Electric Power Co. executives were indicted on the grounds of criminal negligence after a citizens' panel forced prosecution. On Mar. 21, in the first of thirty lawsuits to be brought by Fukushima evacuees, a court in Japan held the Japanese government and Tepco liable for negligence in failing to take adequate measures to prevent the triple reactor meltdowns.

(continued on page 2)

Perspective *(continued from page 1)*

Fukushima is a stark reminder that the public will demand accountability when it comes to preventable disasters, particularly one involving nuclear and poor governance, as Fukushima was deemed a man-made disaster.

At the London roundtable, the discussion was animated and, while disagreements reigned, on two things all agreed: while events causing a radiological release are not specifically excluded under the regimes, cyber insurance needs to be further developed to cover non-radiological but potentially catastrophic events; and operators can protect themselves by demonstrating exemplary safety and security practices not only to ensure safe and secure operations but also to avoid or armor themselves in the event of lawsuits. Regulatory compliance is a minimum and not enough to defend against litigation.

For under-insured cyber risks, development and adoption of an agreed good governance approach are especially important to demonstrate owner/operator reasonable conduct.

With appropriate demonstration of risk management, insurers may be willing to provide higher caps and/or more accurately priced and structured policies — in conventional policies and in nuclear policies inside the liability regimes. This is an important factor in the near term as changes in international treaties or domestic regimes to cover events, such as those that are cyber- or terrorist-related, can take decades. Efforts are now underway to better define what is expected of the industry — from operators to insurers. The 2016 Nuclear Industry Summit proposed a good governance template on security, and as part of a follow-on to that effort the Stimson Center and WINS hope to develop an industry-agreed governance template for security, including cybersecurity, later this year working with the Nuclear Industry Steering Group for Security. The effectiveness of such a template will ultimately be judged by the courts and the larger court of public opinion. ☞